EC441: Lab 6

Daniel Andronov

Monday 21$^{\text{st}}$ November, 2016

6.0 Prelab

Problem 4.5

Part a)

Prefix	Interface
224.0.0.0	0
224.64.0.0	1
224.65.0.0	2
225.64.0.0	3
else	4

Part b)

- **i)** 200.145.81.85 matches no prefix and is sent to interface 3
- **i)** 225.64.195.60 matches 225.0.0.0 the most and is sent to interface 1
- **i)** 225.128.17.119 matches no prefix and is sent to interface 3

Problem 4.6

Range	Interface
0 - 63	0
64 - 95	1
96 - 127	2
128 - 192	3
192 - 255	4

Problem 4.8 Subnet 1 needs 12 interfaces which requires 3 bits. Subnets 2 need 60 interfaces or 6 bits and Subnet 3 needs 7 bits for 90 interfaces.

Subnet	Network Address
1	223.1.170.240/3
2	223.1.17.192/6
3	223.1.17.128/9

Problem 4.17

Part a) Capture packets & continually update the max range of the IDENT field, thereby counting the number of hosts being the NAT

Part b) The IDENT field is randomly assigned the above method would not work, instead the number of unique IDENT's should be counted to indentify the number of hosts behind a NAT

6.2 ICMP and Ping

Problem 1

Part a) Host IP addr. : `172.16.199132`.

Part b) Dest IP addr. : `143.89.14.2`.

Part c) ICMP protocol No.: 1.

Part d) ICMP is not an application layer protocol, and only communicates between hosts and routers.

Part e) ICMP type: 8 and code: 0. The type indicates that this ICMP is a ping request and the code means ??

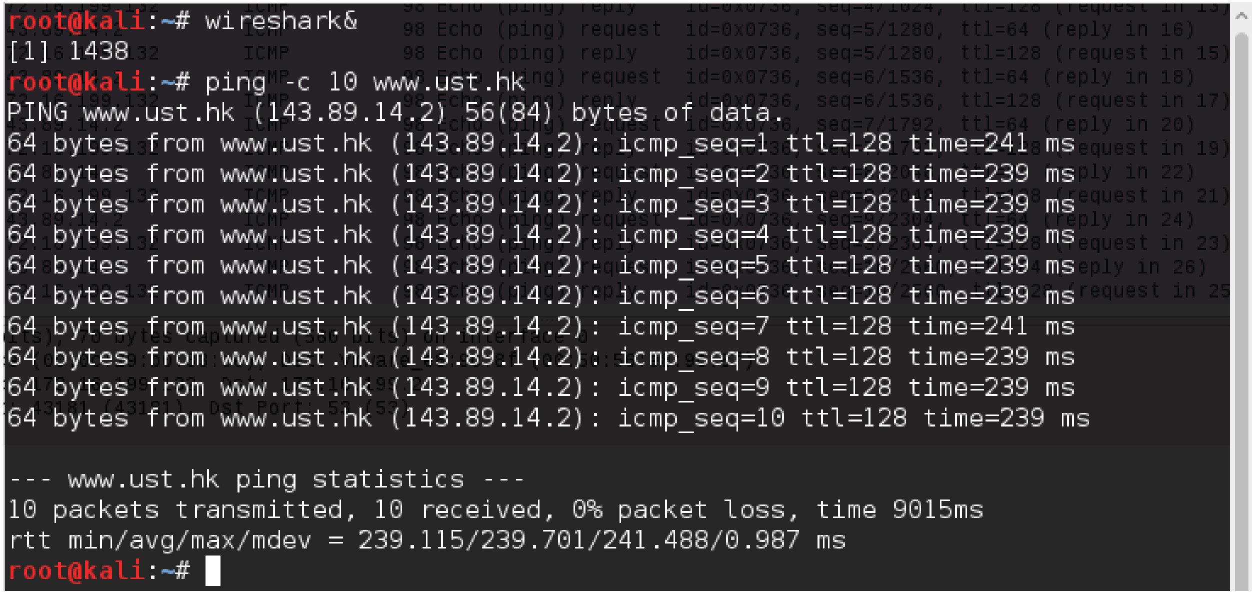
Part f) Sequence No.: (BE)1, (LE)256. Identifier: (BE):1846, (LE):13831. The sequence number and indetifier are used to match responses to their request.

Problem 2

Part a) Type: 0, Code: 0. This pair of values correspond to a ICMP ping reply message

Part b) Sequence Number: (BE)1 & (LE) 256, Identifier: (BE)1846 & (LE)13831. The sequence number and indetifier are used to match responses to their request.

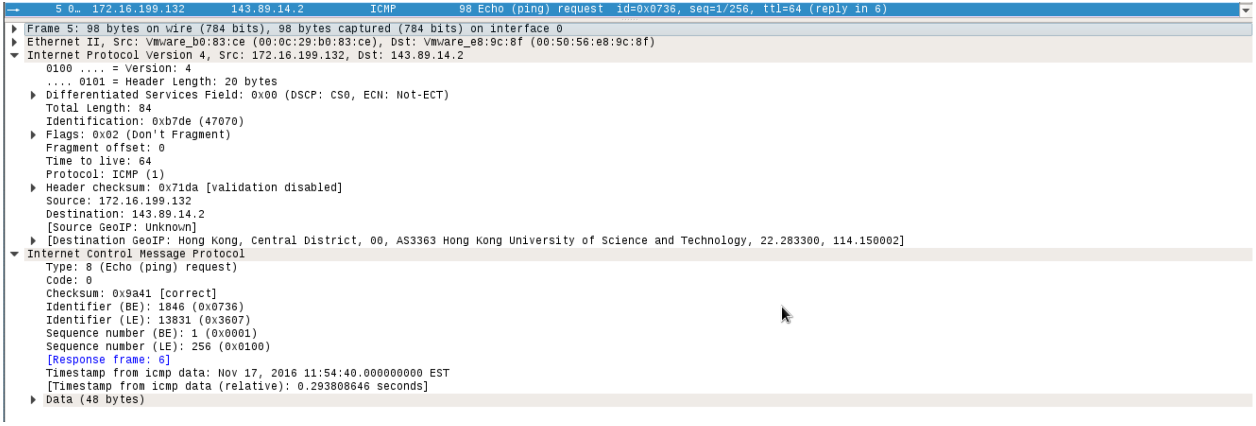
Figure 1: The console output of the ping to ust.hk



```
root@kali:~# wireshark&
[1] 1438
root@kali:~# ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.2) 56(84) bytes of data.
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=1 ttl=128 time=241 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=2 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=3 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=4 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=5 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=6 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=7 ttl=128 time=241 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=8 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=9 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=10 ttl=128 time=239 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 239.115/239.701/241.488/0.987 ms
root@kali:~# 
```

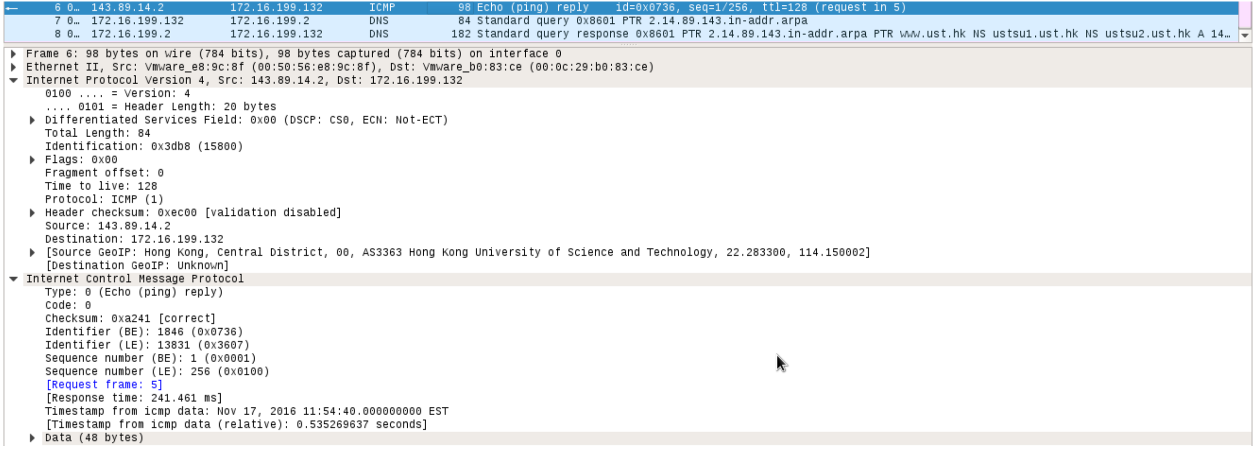
Figure 2: The first ICMP packet



```
→   5 0…  172.16.199.132     143.89.14.2       ICMP       98 Echo (ping) request  id=0x0736, seq=1/256, ttl=64 (reply in 6)

▶ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
▼ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 143.89.14.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0xb7de (47070)
   ▶ Flags: 0x02 (Don't Fragment)
     Fragment offset: 0
     Time to live: 64
     Protocol: ICMP (1)
   ▶ Header checksum: 0x71da [validation disabled]
     Source: 172.16.199.132
     Destination: 143.89.14.2
     [Source GeoIP: Unknown]
   ▶ [Destination GeoIP: Hong Kong, Central District, 00, AS3363 Hong Kong University of Science and Technology, 22.283300, 114.150002]
▼ Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0x9a41 [correct]
     Identifier (BE): 1846 (0x0736)
     Identifier (LE): 13831 (0x3607)
     Sequence number (BE): 1 (0x0001)
     Sequence number (LE): 256 (0x0100)
     [Response frame: 6]
     Timestamp from icmp data: Nov 17, 2016 11:54:40.000000000 EST
     [Timestamp from icmp data (relative): 0.293808646 seconds]
   ▶ Data (48 bytes)
```

Figure 3: The ICMP reply to the first packet



```
←   6 0…  143.89.14.2        172.16.199.132    ICMP       98 Echo (ping) reply    id=0x0736, seq=1/256, ttl=128 (request in 5)
    7 0…  172.16.199.132     172.16.199.2      DNS        84 Standard query 0x8601 PTR 2.14.89.143.in-addr.arpa
    8 0…  172.16.199.2       172.16.199.132    DNS       182 Standard query response 0x8601 PTR 2.14.89.143.in-addr.arpa PTR www.ust.hk NS ustsu1.ust.hk NS ustsu2.ust.hk A 14…

▶ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Vmware_e8:9c:8f (00:50:56:e8:9c:8f), Dst: Vmware_b0:83:ce (00:0c:29:b0:83:ce)
▼ Internet Protocol Version 4, Src: 143.89.14.2, Dst: 172.16.199.132
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0x3db8 (15800)
   ▶ Flags: 0x00
     Fragment offset: 0
     Time to live: 128
     Protocol: ICMP (1)
   ▶ Header checksum: 0xec00 [validation disabled]
     Source: 143.89.14.2
     Destination: 172.16.199.132
   ▶ [Source GeoIP: Hong Kong, Central District, 00, AS3363 Hong Kong University of Science and Technology, 22.283300, 114.150002]
     [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
     Type: 0 (Echo (ping) reply)
     Code: 0
     Checksum: 0xa241 [correct]
     Identifier (BE): 1846 (0x0736)
     Identifier (LE): 13831 (0x3607)
     Sequence number (BE): 1 (0x0001)
     Sequence number (LE): 256 (0x0100)
     [Request frame: 5]
     [Response time: 241.461 ms]
     Timestamp from icmp data: Nov 17, 2016 11:54:40.000000000 EST
     [Timestamp from icmp data (relative): 0.535269637 seconds]
   ▶ Data (48 bytes)
```

6.3 ICMP and Traceroute

Problem 1

Part a) Host IP addr.: `172.16.199.132`.

Part b) Dest IP addr.: `222.92.46.5`.

Part c) UDP protocol No.: 17.

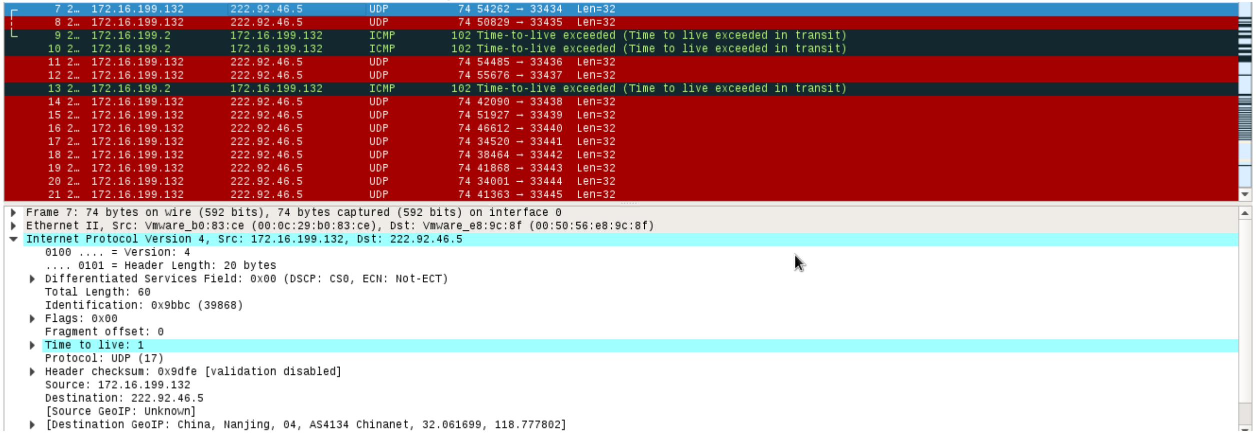
Part d) TTL field value: 1

Problem 2 The fourth UDP packet had a TTL of 2.

Problem 3 The ICMP TTL-exceeded error has type 11, code 0 field values

Problem 4 ??

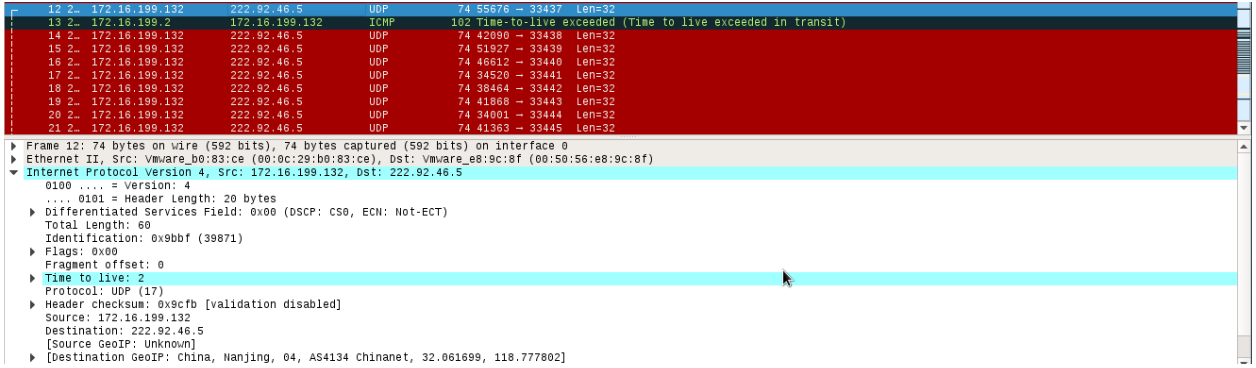
Figure 4: The first UDP packet



```
  7 2…  172.16.199.132    222.92.46.5       UDP        74 54262 → 33434  Len=32
  8 2…  172.16.199.132    222.92.46.5       UDP        74 50829 → 33435  Len=32
  9 2…  172.16.199.2      172.16.199.132    ICMP      102 Time-to-live exceeded (Time to live exceeded in transit)
 10 2…  172.16.199.2      172.16.199.132    ICMP      102 Time-to-live exceeded (Time to live exceeded in transit)
 11 2…  172.16.199.132    222.92.46.5       UDP        74 54485 → 33436  Len=32
 12 2…  172.16.199.132    222.92.46.5       UDP        74 55676 → 33437  Len=32
 13 2…  172.16.199.2      172.16.199.132    ICMP      102 Time-to-live exceeded (Time to live exceeded in transit)
 14 2…  172.16.199.132    222.92.46.5       UDP        74 42090 → 33438  Len=32
 15 2…  172.16.199.132    222.92.46.5       UDP        74 51927 → 33439  Len=32
 16 2…  172.16.199.132    222.92.46.5       UDP        74 46612 → 33440  Len=32
 17 2…  172.16.199.132    222.92.46.5       UDP        74 34520 → 33441  Len=32
 18 2…  172.16.199.132    222.92.46.5       UDP        74 38464 → 33442  Len=32
 19 2…  172.16.199.132    222.92.46.5       UDP        74 41868 → 33443  Len=32
 20 2…  172.16.199.132    222.92.46.5       UDP        74 34001 → 33444  Len=32
 21 2…  172.16.199.132    222.92.46.5       UDP        74 41363 → 33445  Len=32
```

```
▶ Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
▼ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x9bbc (39868)
  ▶ Flags: 0x00
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
  ▶ Header checksum: 0x9dfe [validation disabled]
    Source: 172.16.199.132
    Destination: 222.92.46.5
    [Source GeoIP: Unknown]
  ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
```

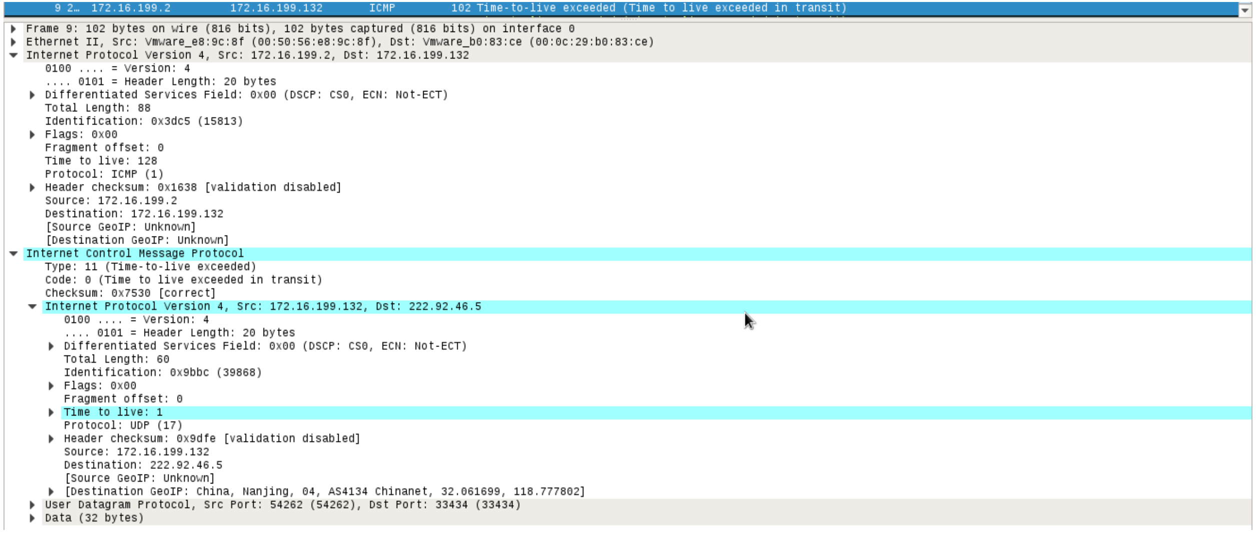
Figure 5: The fourth UDP packet



```
 12 2…  172.16.199.132    222.92.46.5       UDP        74 55676 → 33437  Len=32
 13 2…  172.16.199.2      172.16.199.132    ICMP      102 Time-to-live exceeded (Time to live exceeded in transit)
 14 2…  172.16.199.132    222.92.46.5       UDP        74 42090 → 33438  Len=32
 15 2…  172.16.199.132    222.92.46.5       UDP        74 51927 → 33439  Len=32
 16 2…  172.16.199.132    222.92.46.5       UDP        74 46612 → 33440  Len=32
 17 2…  172.16.199.132    222.92.46.5       UDP        74 34520 → 33441  Len=32
 18 2…  172.16.199.132    222.92.46.5       UDP        74 38464 → 33442  Len=32
 19 2…  172.16.199.132    222.92.46.5       UDP        74 41868 → 33443  Len=32
 20 2…  172.16.199.132    222.92.46.5       UDP        74 34001 → 33444  Len=32
 21 2…  172.16.199.132    222.92.46.5       UDP        74 41363 → 33445  Len=32
```

```
▶ Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
▼ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x9bbf (39871)
  ▶ Flags: 0x00
    Fragment offset: 0
  ▶ Time to live: 2
    Protocol: UDP (17)
  ▶ Header checksum: 0x9cfb [validation disabled]
    Source: 172.16.199.132
    Destination: 222.92.46.5
    [Source GeoIP: Unknown]
  ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
```

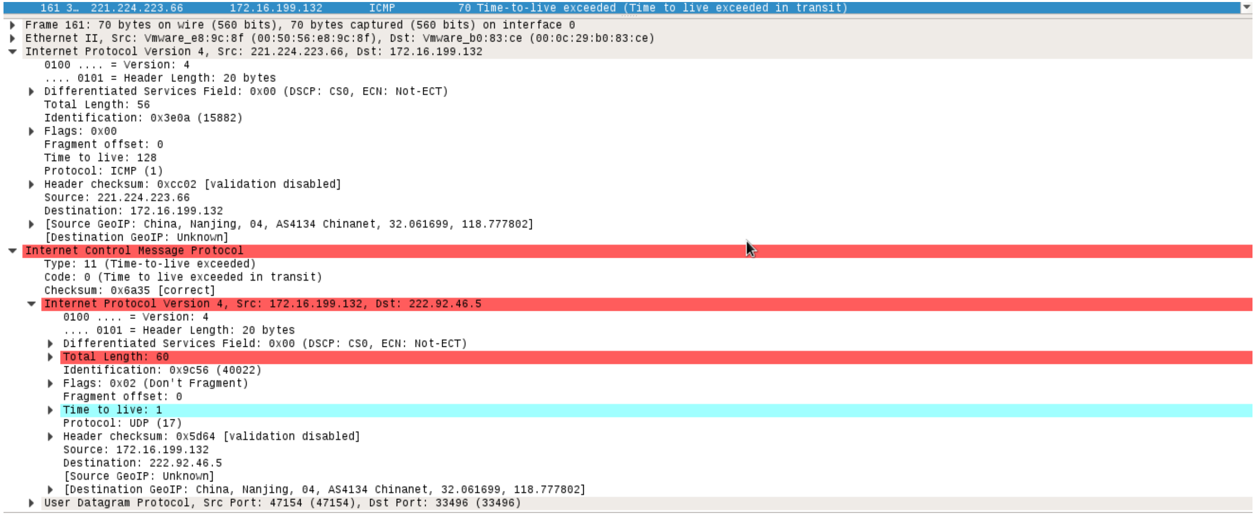
Figure 6: The ICMP TTL-exceeded packet



```
  9 2…  172.16.199.2      172.16.199.132    ICMP      102 Time-to-live exceeded (Time to live exceeded in transit)
```

```
▶ Frame 9: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
▶ Ethernet II, Src: Vmware_e8:9c:8f (00:50:56:e8:9c:8f), Dst: Vmware_b0:83:ce (00:0c:29:b0:83:ce)
▼ Internet Protocol Version 4, Src: 172.16.199.2, Dst: 172.16.199.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x3dc5 (15813)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ▶ Header checksum: 0x1638 [validation disabled]
    Source: 172.16.199.2
    Destination: 172.16.199.132
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x7530 [correct]
  ▼ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
      Identification: 0x9bbc (39868)
    ▶ Flags: 0x00
      Fragment offset: 0
    ▶ Time to live: 1
      Protocol: UDP (17)
    ▶ Header checksum: 0x9dfe [validation disabled]
      Source: 172.16.199.132
      Destination: 222.92.46.5
      [Source GeoIP: Unknown]
    ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
  ▶ User Datagram Protocol, Src Port: 54262 (54262), Dst Port: 33434 (33434)
  ▶ Data (32 bytes)
```

Figure 7:



```
  161 3…  221.224.223.66       172.16.199.132       ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
▶ Frame 161: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Vmware_e8:9c:8f (00:50:56:e8:9c:8f), Dst: Vmware_b0:83:ce (00:0c:29:b0:83:ce)
▼ Internet Protocol Version 4, Src: 221.224.223.66, Dst: 172.16.199.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x3e0a (15882)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ▶ Header checksum: 0xcc02 [validation disabled]
    Source: 221.224.223.66
    Destination: 172.16.199.132
  ▶ [Source GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6a35 [correct]
  ▼ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    ▶ Total Length: 60
      Identification: 0x9c56 (40022)
    ▶ Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
    ▶ Time to live: 1
      Protocol: UDP (17)
    ▶ Header checksum: 0x5d64 [validation disabled]
      Source: 172.16.199.132
      Destination: 222.92.46.5
      [Source GeoIP: Unknown]
    ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
  ▶ User Datagram Protocol, Src Port: 47154 (47154), Dst Port: 33496 (33496)
```

6.4 Fragmentation

Problem 1 No fragrments and as no packet as the MF field set.

Problem 2 Yes, the MF bit is set and the 1st packet. There are 2 fragments in the form of UDP packets

Problem 3 Yes, there are 3 fragments.

Problem 4 THe MF field is sen and the lenght of the packet is of maximum size. Also, the offset is 0.

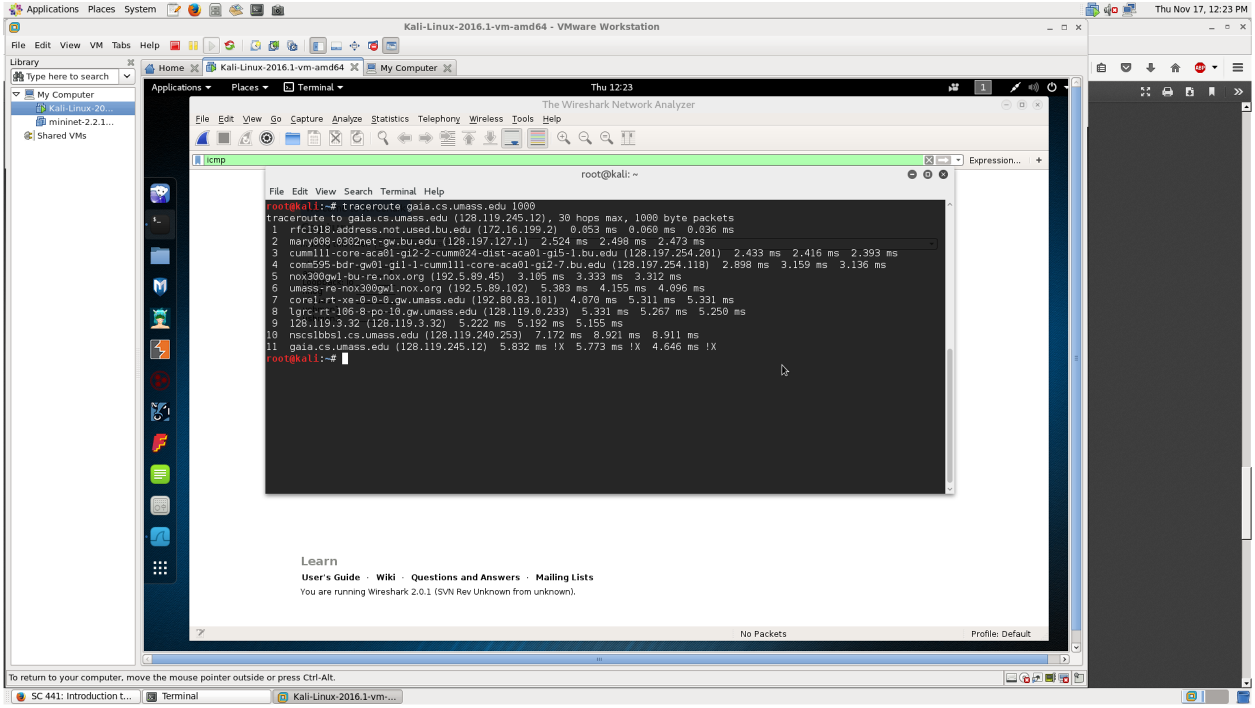
Problem 5 The MF field is 1 and the offset is 1480.

Problem 6 The offset and the checksum.

Problem 7 All Flags are set to 0 and the sum of the offset and packet length adds to the original datagram size.

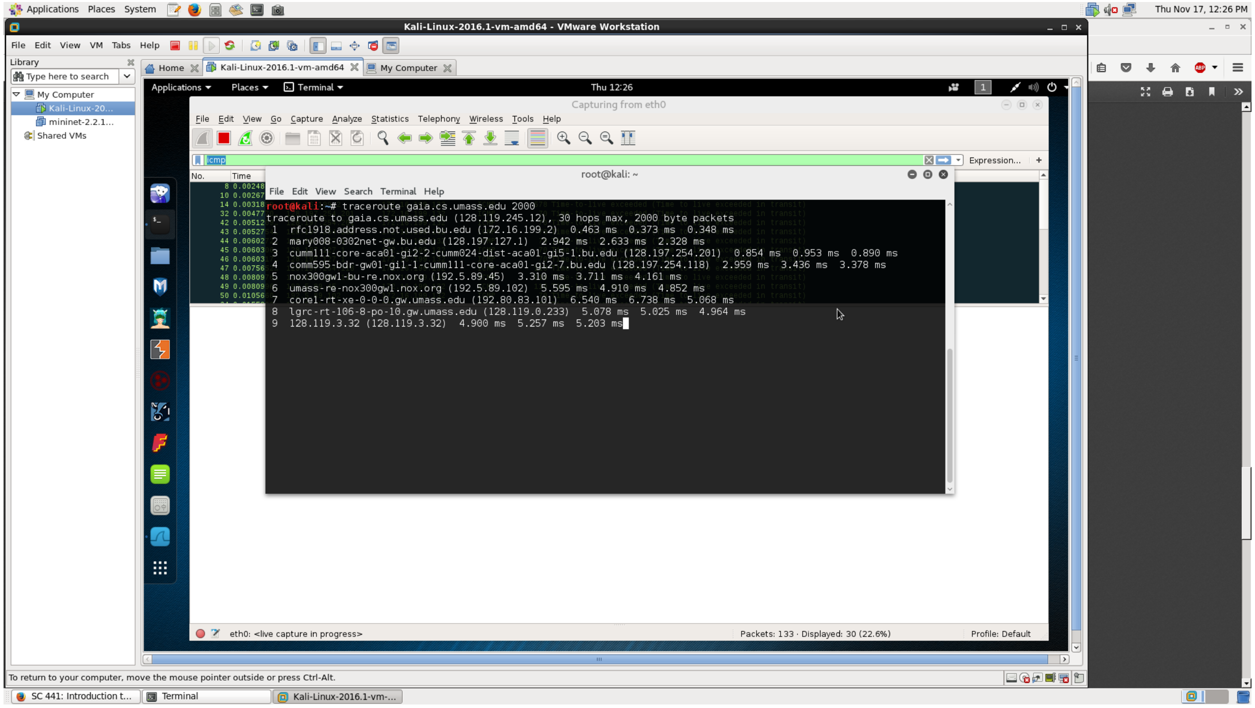
Problem 8 The MTU of the network is 1500 bytes.

Figure 8: Console output for ping with datagram of 1000B



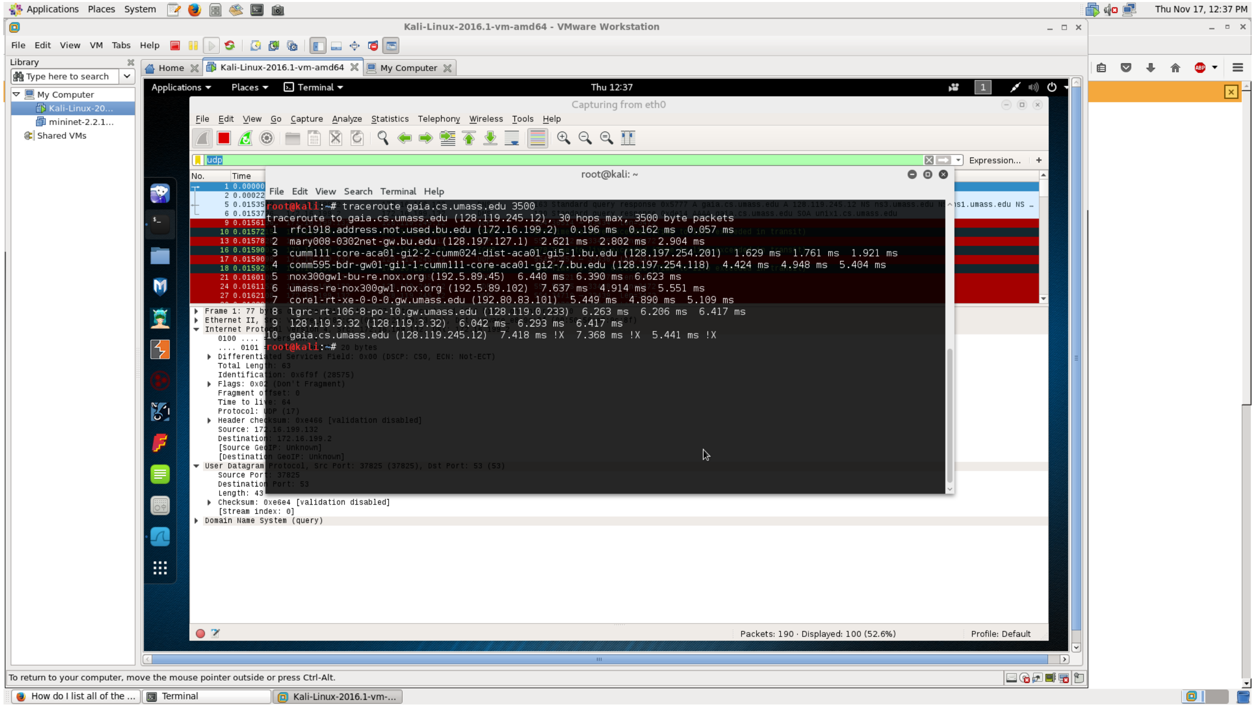
```
root@kali:~# traceroute gaia.cs.umass.edu 1000
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 1000 byte packets
 1  rfc1918.address.not.used.bu.edu (172.16.199.2)  0.053 ms  0.060 ms  0.036 ms
 2  mary008-0302net-gw.bu.edu (128.197.127.1)  2.524 ms  2.498 ms  2.473 ms
 3  cumm111-core-aca01-gi2-2-cumm024-dist-aca01-gi5-1.bu.edu (128.197.254.201)  2.433 ms  2.416 ms  2.393 ms
 4  comm595-bdr-gw01-gi1-1-cumm111-core-aca01-gi2-7.bu.edu (128.197.254.118)  2.898 ms  3.159 ms  3.136 ms
 5  nox300gw1-bu-re.nox.org (192.5.89.45)  3.105 ms  3.333 ms  3.312 ms
 6  umass-re-nox300gw1.nox.org (192.5.89.102)  5.383 ms  4.155 ms  4.096 ms
 7  core1-rt-xe-0-0-0.gw.umass.edu (192.80.83.101)  4.070 ms  5.311 ms  5.331 ms
 8  lgrc-rt-106-8-po-10.gw.umass.edu (128.119.0.233)  5.331 ms  5.267 ms  5.250 ms
 9  128.119.3.32 (128.119.3.32)  5.222 ms  5.192 ms  5.155 ms
10  nscs1bbs1.cs.umass.edu (128.119.240.253)  7.172 ms  8.921 ms  8.911 ms
11  gaia.cs.umass.edu (128.119.245.12)  5.832 ms !X  5.773 ms !X  4.646 ms !X
root@kali:~# 
```

Figure 9: Console output for ping with datagram of 2000B



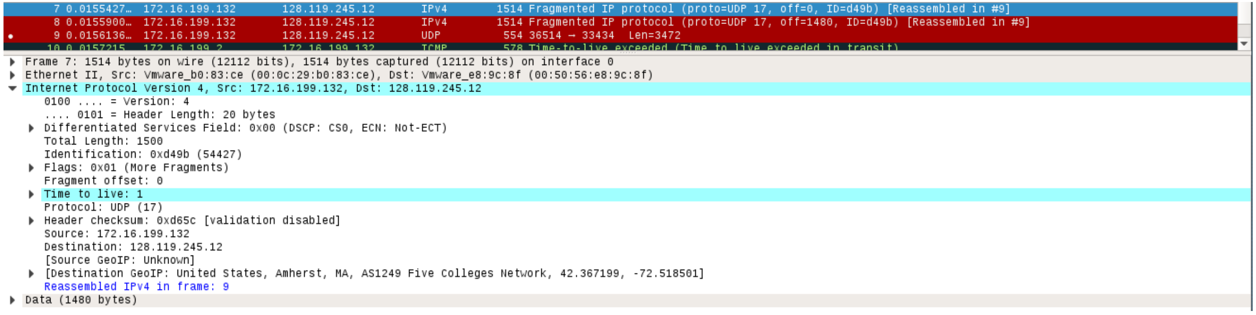
```
root@kali:~# traceroute gaia.cs.umass.edu 2000
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 2000 byte packets
 1  rfc1918.address.not.used.bu.edu (172.16.199.2)  0.463 ms  0.373 ms  0.348 ms
 2  mary008-0302net-gw.bu.edu (128.197.127.1)  2.942 ms  2.633 ms  2.328 ms
 3  cumm111-core-aca01-gi2-2-cumm024-dist-aca01-gi5-1.bu.edu (128.197.254.201)  0.854 ms  0.953 ms  0.890 ms
 4  comm595-bdr-gw01-gi1-1-cumm111-core-aca01-gi2-7.bu.edu (128.197.254.118)  2.959 ms  3.436 ms  3.378 ms
 5  nox300gw1-bu-re.nox.org (192.5.89.45)  3.310 ms  3.711 ms  4.161 ms
 6  umass-re-nox300gw1.nox.org (192.5.89.102)  5.595 ms  4.910 ms  4.852 ms
 7  core1-rt-xe-0-0-0.gw.umass.edu (192.80.83.101)  6.540 ms  6.738 ms  5.068 ms
 8  lgrc-rt-106-8-po-10.gw.umass.edu (128.119.0.233)  5.078 ms  5.025 ms  4.964 ms
 9  128.119.3.32 (128.119.3.32)  4.900 ms  5.257 ms  5.203 ms
```

Figure 10: Console output for ping with datagram of 3500B


Applications Places System
Thu Nov 17, 12:37 PM
Kali-Linux-2016.1-vm-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali-Linux-20...
mininet-2.2.1...
Shared VMs
Home
Kali-Linux-2016.1-vm-amd64
My Computer
Applications Places Terminal
Thu 12:37
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
root@kali: ~
File Edit View Search Terminal Help
Packets: 190 · Displayed: 100 (52.6%)
Profile: Default
To return to your computer, move the mouse pointer outside or press Ctrl-Alt.
How do I list all of the ...
Terminal
Kali-Linux-2016.1-vm-...

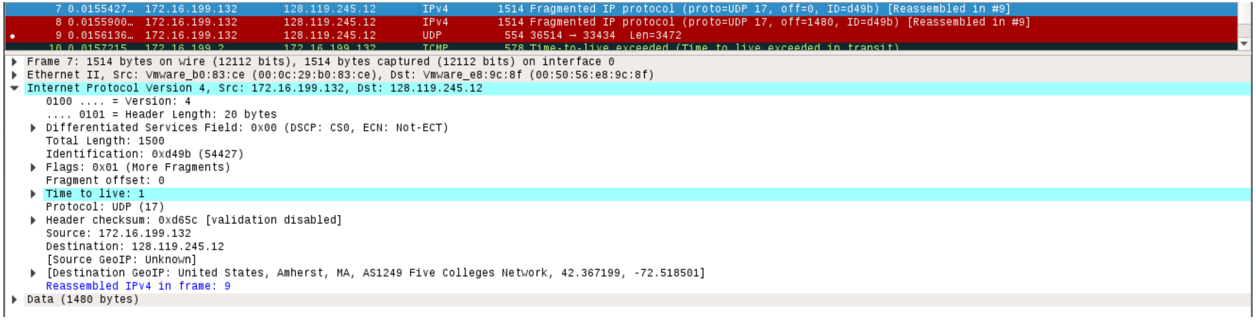
```
root@kali:~# traceroute gaia.cs.umass.edu 3500
traceroute to gaia.cs.umass.edu (128.119.245.12), 30 hops max, 3500 byte packets
 1  rfc1918.address.not.used.bu.edu (172.16.199.2)  0.196 ms  0.162 ms  0.057 ms
 2  mary008-0302net-gw.bu.edu (128.197.127.1)  2.621 ms  2.802 ms  2.904 ms
 3  cumm111-core-aca01-gi2-2-cumm024-dist-aca01-gi5-1.bu.edu (128.197.254.201)  1.629 ms  1.761 ms  1.921 ms
 4  comm595-bdr-gw01-gi1-1-cumm111-core-aca01-gi2-7.bu.edu (128.197.254.118)  4.424 ms  4.948 ms  5.404 ms
 5  nox300gw1-bu-re.nox.org (192.5.89.45)  6.440 ms  6.390 ms  6.623 ms
 6  umass-re-nox300gw1.nox.org (192.5.89.102)  7.637 ms  4.914 ms  5.551 ms
 7  core1-rt-xe-0-0-0.gw.umass.edu (192.80.83.101)  5.449 ms  4.890 ms  5.109 ms
 8  lgrc-rt-106-8-po-10.gw.umass.edu (128.119.0.233)  6.263 ms  6.206 ms  6.417 ms
 9  128.119.3.32 (128.119.3.32)  6.042 ms  6.293 ms  6.417 ms
10  gaia.cs.umass.edu (128.119.245.12)  7.418 ms !X  7.368 ms !X  5.441 ms !X
root@kali:~#
```

Figure 11: First UDP probe



```
    7 0.0155427…  172.16.199.132     128.119.245.12     IPv4       1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=d49b) [Reassembled in #9]
    8 0.0155900…  172.16.199.132     128.119.245.12     IPv4       1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=d49b) [Reassembled in #9]
•   9 0.0156136…  172.16.199.132     128.119.245.12     UDP         554 36514 → 33434  Len=3472
   10 0.0157215   172.16.199.2       172.16.199.132     ICMP        578 Time-to-live exceeded (Time to live exceeded in transit)
▸ Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
▾ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xd49b (54427)
  ▸ Flags: 0x01 (More Fragments)
    Fragment offset: 0
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0xd65c [validation disabled]
    Source: 172.16.199.132
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
  ▸ [Destination GeoIP: United States, Amherst, MA, AS1249 Five Colleges Network, 42.367199, -72.518501]
    Reassembled IPv4 in frame: 9
▸ Data (1480 bytes)
```

Figure 12: Second UDP fragment



```
    7 0.0155427…  172.16.199.132     128.119.245.12     IPv4       1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=d49b) [Reassembled in #9]
    8 0.0155900…  172.16.199.132     128.119.245.12     IPv4       1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=d49b) [Reassembled in #9]
•   9 0.0156136…  172.16.199.132     128.119.245.12     UDP         554 36514 → 33434  Len=3472
   10 0.0157215   172.16.199.2       172.16.199.132     ICMP        578 Time-to-live exceeded (Time to live exceeded in transit)
▸ Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
▾ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xd49b (54427)
  ▸ Flags: 0x01 (More Fragments)
    Fragment offset: 0
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0xd65c [validation disabled]
    Source: 172.16.199.132
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
  ▸ [Destination GeoIP: United States, Amherst, MA, AS1249 Five Colleges Network, 42.367199, -72.518501]
    Reassembled IPv4 in frame: 9
▸ Data (1480 bytes)
```